

REMARKS

The Applicants request reconsideration of the rejection.

Claims 1-25 are now canceled in favor of new claims 26-29.

Claims 1-3, 6, 8-10, 12, 15-16, 19, and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Belani, et al., US 6,772,350 (Belani) in view of Chang, et al., US 2003/0229623 (Chang). The Applicants traverse as follows.

A notable feature of the present invention is that, in response to a request for changing the permission attribute for an operation for an information item related to a user, communicated through a user terminal, a server changes the permission attribute for the operation or information item for a higher layer on the basis of the content of the request, the hierarchy of operations, and the hierarchy of information items.

As claimed in claim 26, and disclosed illustratively in Fig. 10, when there is a request from the user terminal to permit executing an open operation, a read operation, or a write operation based on identification information, location information, or communication status of the user terminal, a control unit changes the permission attribute from non-permission to permission, and refers to the layer of operation to be requested for changing the permission to determine whether there is a layer having a level higher than that for the operation requested. If so, then the control unit sets the permission attribute of the higher-level operation to be that of the operation layer of concern. A similar determination and setting is made for the information of the user terminal.

Neither Belani nor Chang suggests this performance. In particular, neither document suggests to change and set an operation permission attribute to that of a

lower-level operation, and an information item permission attribute to that of a lower-level information item.

The Office Action would find similar limitations in the concept of "reverse inheritance" as disclosed by Chang in Fig. 8b and paragraphs [0113] and [0116]. However, the most readily apparent flaw in citing Chang with Belani is that Belani relies on searching upward in a hierarchy to find permissions that float downward. That is, when permissions attached to requested operations or resources cannot be resolved for a user making a request, resolution is sought by proceeding up the user's and/or resource's hierarchy information to find a higher permission level that can be applied to the lower-level user/resource. This is the opposite of the path taught by Chang, and such a mutual teaching away prevents the asserted combination in a rejection under §103.

In addition, the approach taken by Chang is different from that of claim 26. In particular, Chang gives, to a user assigned to a security role for a specific topic, the same security role for all topics that are ancestors of the specific topic for which the role is assigned. Chang does not teach to "climb" the hierarchical ladder to reassign a permission, but universally applies the security role according to a specific assignment of concern.

Thus, independent claim 26 is free of Belani and Chang taken individually or in combination with any other reference of record, including their own "combination" which is made unreasonable by their own teachings, as discussed above.

Further, dependent claims 27-29 inherit the patentable features of claim 26 from which each is derived, and thus their separate patentability will not be argued at this time, for brevity.

In view of the foregoing amendments and remarks, the Applicants request reconsideration of the rejection and allowance of the claims.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Brundidge & Stanger, P.C., Deposit Account No. 50-4888 (referencing attorney docket no. NIT-415).

Respectfully submitted,

BRUNDIDGE & STANGER, P.C.

/Daniel J. Stanger/
Daniel J. Stanger
Registration No. 32,846

DJS/
(703) 684-1470